Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
Amendments to Part 4 of the Commission's Rules Concerning Disruptions to Communications	)	PS Docket No. 15-80

COMMENTS OF AT&T

AT&T Services, Inc., on behalf of itself and its affiliates (collectively, "AT&T"), submits these comments in response to the Federal Communications Commission's ("FCC" or "Commission") *Second Further Notice of Proposed Rulemaking*[1] soliciting input on an information sharing framework to provide state and federal agencies with access to Network Outage Reporting System ("NORS") and Disaster Information Reporting System ("DIRS") information.

I. INTRODUCTION

AT&T supports the Commission's initiative to aid the Nation's emergency response efforts and incident preparedness goals. AT&T submits outage reports to NORS as required and infrastructure status reports to DIRS to enable the Commission to evaluate network reliability. AT&T agrees that federal, state and Tribal Nation governments ("government agencies") could benefit from direct access to certain outage data submitted to NORS and DIRS in preparation for and during emergencies (including disasters), provided the information sharing process is implemented with appropriate safeguards. First, information sharing should be limited to the information that would directly facilitate emergency preparedness and response. The use of the

[1] Amendments to Part 4 of the Commission's Rules Concerning Disruptions to Communications, *Second Further Notice of Proposed Rulemaking*, PS Docket No. 15-80, FCC 20-20 (Mar. 2, 2020) ("*FNPRM*").

data should be strictly limited to these purposes and extraneous information submitted in NORS and DIRS should not be shared outside the FCC with other government agencies. Second, the Commission must carefully consider how to aggregate and anonymize carrier-submitted data, which may be proprietary or sensitive, before sharing with the public. Some types of data may be well suited to anonymization through aggregation while other types of data should not be shared at all. Third, if the Commission decides to adopt an information sharing regime similar to the proposals in its *FNPRM*, the implementation process for this new framework must resolve various concerns regarding the content and format of information to be shared, as well as the method of accessing such information. Procedures should ensure that potential recipients have a "need to know" basis for access to the information and understand their responsibilities for maintaining confidentiality.

II. THE INFORMATION SHARED WITH GOVERNMENT AGENCIES SHOULD BE LIMITED TO THAT WHICH WOULD FACILITATE EMERGENCY PREPAREDNESS AND RESPONSE.

The NORS/DIRS information to be shared with government agencies should be limited to information needed for emergency preparedness and response. Government agencies have an interest in access to certain network outage data in order to prepare for and respond to a range of emergencies, including natural or other disasters, that could affect the populations of their jurisdictions. During times of crisis, communications networks are critical links for first responders, the public, and government agencies to maintain ongoing situational awareness and coordinate responses. In the current pandemic, the networks of AT&T and other providers make it possible for the public to be informed, engaged with telemedicine and distance education, connected to loved ones, entertained, and in many cases, employed. More than ever, these assets are critical infrastructure and government agencies, in some cases, could benefit from access to timely and effective information about networks and services needed in emergencies.

Access, however, must be narrowly tailored to the information needed to fulfill that legitimate purpose. Much of the information contained in NORS/DIRS reports is of a competitive and/or national security nature and must be properly safeguarded by all government agencies that access the data. In no event should network outage data provided for these purposes be taken out of context and used for non-emergency-related regulatory purposes, such as (but not limited to) merger review, consumer protection activities, or release of competitive information (even aggregated) to the public. There are other regulatory and commercially available tools (such as transaction-specific data requests and commercial industry analysis reports) that are well-suited to obtaining that type of information and provide the proper context for regulatory activities outside of emergency preparedness and response. Shared NORS/DIRS data should in no way be used to micromanage network deployment decisions by providers within a jurisdiction. Using network outage reporting data in these ways—for purposes well beyond those for which it was designed—could lead regulators and consumers to inaccurate and unfair conclusions about a particular provider and could create disincentives for candid disclosures of network conditions, thereby subverting the initial purpose for this data collection.

Moreover, some information contained in NORS or DIRS submissions is not relevant to emergency preparedness and response, and/or contains highly confidential information about providers' operations, personnel, and network equipment locations. As a result, certain categories of information submitted to NORS/DIRS should not be shared, even on a confidential basis, with government agencies. First, individual carrier maps and the underlying data and shape files submitted via NORS/DIRS should *not* be shared with any government agencies or the public. The carrier shape files used to generate the maps submitted contain the most detailed information about carrier networks and are proprietary and highly competitively sensitive.

Disclosure of such detailed network information endangers network security by vandals or other malicious actors.[2] Making the most sensitive network information available in a single place to many recipients, thereby increasing possible points of disclosure, would substantially increase risk that a hostile actor could obtain that information and use it to attack critical infrastructure. Even the risk of inadvertent disclosure by a government agency outweighs any benefit of sharing this most sensitive information. If, however, the Commission does determine that sharing such network data would be in the public interest, it must address these risks by implementing effective safeguards, such as aggregating and anonymizing the data before disclosure.

Second, information sharing should not include disclosure of the contact information of personnel responsible for filing the NORS or DIRS report. These staff members are not designated as the points of contact for fielding inquiries from multiple agencies across dozens of jurisdictions, and therefore, should not be subject to disclosure of their names and contact information.

Third, root cause analysis of network outages should also be excluded. Detailed root cause analysis is a backward-looking activity that is normally completed well after the outage has been resolved and thus is of little use in preparing for and responding to an emergency. Restoration is appropriately the priority during any network outage caused by or occurring during an emergency. Moreover, root cause analysis commonly includes highly sensitive competitive information regarding the provider's vendor services or products, operational procedures, and network details. Disclosure of this information could be competitively damaging and could even potentially pose a national security risk (depending on the details of

[2] *See* New York Times, "Burning Cell Towers, Out of Baseless Fears They Spread the Virus," https://www.nytimes.com/2020/04/10/technology/coronavirus-5g-uk.html (Apr. 10, 2020).

any particular root cause analysis). For these reasons, these types of information should not be routinely disclosed.

III. THE COMMISSION SHOULD AVOID DISCLOSURE OF CONFIDENTIAL INFORMATION TO THE PUBLIC.

Any disclosure of DIRS/NORS information to the public must be subject to safeguards to ensure that information provides benefit to the public without disclosure of identifiable, confidential details. In many cases, the general public would not have sufficient expertise to accurately and fairly assess a particular carrier's network performance based on the data contained in the reports. Disclosure to the public could unnecessarily cause competitive harm and even mislead consumers. Details that pose security risks to critical infrastructure must be withheld. Before disclosure, the Commission must carefully weigh any potential benefit to the public against the risks of disclosure. If the risks exceed the benefit, the Commission should not permit disclosure. If disclosure is in the public interest, the Commission must ensure safeguards strong enough to mitigate any risks, such as aggregating and anonymizing the data before disclosure.

In some cases, aggregation of data among at least four carriers, as the Commission suggests,[3] could be an appropriate mechanism to provide useful information to the public while still protecting confidential data submitted by providers. For example, the FCC compiles public reports on communications status during DIRS activation periods using aggregated data.[4] This

---

[3] *See FNPRM* at ¶ 45 (defining "aggregated NORS and DIRS information" to refer to information from the NORS and DIRS filings of at least four service providers that has been aggregated and anonymized to avoid identifying any service providers by name or in substance).

[4] *See* FCC, Public Safety and Homeland Security Bureau, Operations and Emergency Management Division, FCC Hurricane Response (Oct. 11, 2018), https://www.fcc.gov/fcc-hurricane-response (presenting a collection of public reports released during DIRS activation periods for recent hurricanes); *FNPRM* ¶ 9 ("The Commission also provides aggregated data, without company-identifying information, to the public during disasters.").

type of disclosure of information about wireless services can work well to provide the public with useable information while safeguarding confidentiality.

In contrast, greater care must be taken with wireline data. In some cases, aggregation will not adequately protect information because there is a far greater correlation between specific providers and service territories than with data pertaining to wireless services, meaning that aggregation of wireline data alone may not have a sufficient anonymizing effect.

For these reasons, the Commission must carefully analyze the different types of data submitted, the value of disclosing such data publicly, and how to best protect such data before any public disclosures occur. If effective safeguards cannot be put in place, the information should not be disclosed.

IV. THE COMMISSION SHOULD SEEK INDUSTRY INPUT ON DATA TO BE DISCLOSED AND THE PROCESS FOR GAINING ACCESS BEFORE MOVING FORWARD.

If confidential NORS/DIRS information is to be shared with government agencies, the Commission should ensure that each potential recipient has a "need to know" basis for access to the information, the recipient understands the duty to maintain confidentiality, and the information will be destroyed in a secure manner when there is no longer a "need to know." The Commission can best accomplish this by designating a "coordinator" responsible for the agency's access to confidential NORS/DIRS information.[5] Once designated, the coordinator would have the ability to approve additional requests for access credentials for personnel from that agency. This approach would allow downstream sharing of information by the coordinator,

[5] A similar procedure has worked well in the context of the 911 Reliability Certification System. In that case, the potential information recipient sends a request to a designated FCC staff member to receive coordinator status and these requests are handled on case-by-case basis. *See* Public Notice, *Public Safety and Homeland Security Bureau Announces Availability of 911 Reliability Certification System for Annual Reliability Certifications*, 34 FCC Rcd 6490 (2019); FCC, Frequently Asked Questions: FCC 911 Reliability Certification, https://apps2.fcc.gov/rcs911/911RCS_FAQ.html.

who would be best positioned to ensure that recipients have a "need to know." In developing procedures for access to this sensitive information, the Commission should take special care in granting access credentials to ensure that unauthorized individuals may not gain access. AT&T is aware of a recent incident in which an unknown third party unsuccessfully attempted to gain access credentials for 911 reliability data under false pretenses by posing as an employee of AT&T. Use of a vetted coordinator for managing access credentials at an agency would help mitigate this risk. Further, the agency coordinator would have responsibility for ensuring that personnel follow appropriate procedures to preserve confidentiality, securely destroying the data and promptly reporting to the Commission any breach of rules or procedures related to the handling of the confidential NORS/DIRS information.

Finally, before initiating agency and public disclosures, the Commission should give providers and government agencies the opportunity to review an example of the information to be made available through this process. It would be useful for the providers that submit information to NORS/DIRS to see a mock-up format, any template, and online access tools to be used so that they have an opportunity to raise any concerns and recommend changes. Similarly, feedback from government agencies would ensure that the Commission's final framework provides the state-specific information sought by these parties, while potentially minimizing multiple operationally redundant reporting regimes across providers' service footprints. Such a collaborative process is most likely to achieve the Commission's dual purposes of giving government agencies useful information while also preserving confidentiality of sensitive data.

V. CONCLUSION

AT&T agrees that sharing NORS/DIRS information with government agencies could, in some cases, provide important benefits. AT&T urges the Commission to implement an information sharing process that effectively safeguards the confidentiality of information

submitted to NORS/DIRS and ensures that only appropriate personnel, on a "need to know" basis, at government agencies receive access to the information only after appropriate vetting.

Respectfully submitted,

By: */s/*

Christi Shewman
Gary L. Phillips
David L. Lawson

AT&T SERVICES, INC.
1120 20th Street, NW
Suite 1000
Washington, DC 20036
(202) 457-3090 – phone

Attorneys for AT&T

Scott D. Delacourt
Katy J. Milner

WILEY REIN LLP
1776 K Street, NW
Washington, DC 20006
(202) 719-7000 – phone
(202) 719-7049 – facsimile

Dated April 30, 2020